REMARKS/ARGUMENTS

Applicants thank the Examiner for consideration of the Information Disclosure Statement filed December 3, 2008. Applicants respectfully request consideration of the Information Disclosure Statement filed by Applicants January 21, 2009.

By this amendment, Claims 1-7, 18-20, 25-27 are amended, Claim 16 is canceled, and Claims 32-40 are added. The amendments to the claims as indicated herein do not add any new matter to this application.

Each issue raised in the Office Action mailed December 8, 2009 ("Office Action") is addressed hereinafter.

CLAIM REJECTIONS—35 U.S.C. § 103

Claims 1-7, 16, 18-31 stand rejected under 35 U.S.C. § 102(a) as allegedly anticipated by U.S. Patent Publication No. 2005/0005017 (herein "*Ptacek*") in view of U.S. Patent Publication No. 2002/0019945 (herein *"Houston"*). Those rejections are respectfully traversed.

CLAIM 1

Present Claim 1 requires:

1. A computer-implemented method of analyzing security events, comprising:

receiving and processing security events from one or more security devices in a network, including grouping the security events into network sessions, each session having an identified source and destination;

causing display of a first graph on a display of a computer system, the first graph representing devices in the network, the devices including the one or more security devices and non-security devices, the displayed first graph including one or more individual device symbols and one or more group device symbols, each individual device symbol representing one of the one or more a security devices and each group device symbol representing a group of non-security devices of the network;

causing display of a first security incident volume indicator on the display that indicates a number of network sessions whose source or destination is at any

member of a group of non-security devices corresponding to a particular group device symbol displayed on the display;

wherein the step of causing display of the first security incident volume indicator includes the step of causing the display to visually highlight the particular group device symbol in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol.

Applicants respectfully submit that at least the above-bolded features of Claim 1 are not taught or in any way rendered obvious by *Ptacek* and *Houston*.

Claim 1 features a display of a "first graph" that includes one or more "individual device symbols" and one or more "group device symbols". Each individual device symbol represents a "security device" from which one or more security events were received. Each group device symbol represents "a group of non-security devices".

The display on which the first graph is displayed also includes display of a "first security incident volume indicator" that "indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to a particular group device symbol displayed on the display." The display visually highlights the particular group device symbol "in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol."

For example, as featured in new Claims 33, 36, and 39, the particular group device symbol is visually highlighted by "causing display of a separate security incident volume indicator substantially adjacent to the particular group device symbol for each one of the number of network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol."

As another example, as featured in new Claims 34, 37, and 40, the particular group device symbol is visually highlighted by "causing a change in the appearance of the particular

group device symbol to indicate the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol."

Support for amendments to Claim 1 and new Claims 33, 34, 36, 37, 39, and 40 can be found in at least paragraphs [0010], [0051], and [0053] of the specification, along with figures 4(a) and 5(a) of the drawings.

The display that is caused to be displayed by the method of Claim 1 presents analysis of the received security events in an intuitive form so that a user can easily discern "hotspots" within a network. In particular, a symbol representing a "hotspot" group of non-security devices is visually highlighted so as to simplify the process for the user of tracking down the sources and destinations of a network attack. Such a method is not taught or in any way suggested by *Ptacek* and *Houston*.

PTACEK AND *HOUSTON* DO NOT SATISFY CLAIM 1 AS A WHOLE

In rejecting Claim 1, the Office Action equates Figure 1 of *Ptacek* with the claimed "graph representing devices in [a] network". Figure 1 of *Ptacek*—**a patent drawing, not a graph on a computer display as claimed**—clearly shows security devices such as firewall 111-4, switch 20-1, and router 18 and non-security devices such as SQL Server 12-2, Host 15, Client 10, and Doc. Server 16 represented with individual device symbols. In contrast, the "first graph" of Claim 1 includes "one or more individual device symbols and one or more **group device symbols**, each individual device symbol representing one of the one or more a security devices and each group device symbol **representing a group of non-security devices**". However, Figure 1 of *Ptacek* includes individual device symbols that represent both security devices and non-security devices. By representing both security devices and non-security devices with individual device symbols, Figure 1 of *Ptacek* does not simplify the process of tracking down the sources and destinations of a network attack. On the contrary–and assuming a skilled person would have used a patent drawing as the basis for a computer display format, which is doubtful and unsupported by any evidence—any display based on Figure 1 of *Ptacek* would complicate

the process for a user of tracking down network attacks because the user could not easily discern security devices from non-security devices based on the symbol used to represent the devices.

Further, nothing in *Ptacek* prohibits a group device symbol such as WAN 22 of Figure 1 from representing both security devices and non-security devices. Thus, *Ptacek* does not suggest the feature embodied in Claim 1 that it would be useful to have "**each** individual device symbol representing one of the one or more a security devices and **each** group device symbol representing a group of non-security devices" so as to simplify the process for the user of tracking down the sources and destinations of a network attack. Consequently, Figure 1 of *Ptacek* does not teach or suggest the claimed "first graph on a display of a computer system" featured in Claim 1.

With regard to other features of Claim 1, the Office Action agrees that *Ptacek* does not clearly teach "causing display, with respect to a group device symbol, of a security incident volume indicator that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol", as featured in Claim 1 as amended by Applicant's response filed September 18, 2008. *Ptacek* also does not teach or suggest the following features of Claim 1 as amended herein:

> causing display of a first security incident volume indicator on the display that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to a particular group device symbol displayed on the display;
>
> wherein the step of causing display of the first security incident volume indicator includes the step of causing the display to visually highlight the particular group device symbol in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol.

The present Office Action contends that any deficiencies of *Ptacek* are accounted for by *Houston* and that the combination of *Ptacek* and *Houston* satisfies Claim 1 as a whole. The Office Action is incorrect.

Houston describes a technique by which a list of "scopes" is presented to the user and the user can select a scope from the list to view events that correspond to the selected scope. (*See e.g.*, Figure 15 of *Houston*.) In *Houston*, a scope is a construct whereby events can be filtered/grouped by source or destination address, event type, or other event attributes. (*Houston*, para. [0046].)

Houston does not describe any sort of technique for visually highlighting a symbol that represents a group of non-security devices to indicate a number of scopes or events whose source or destination is at any member of the group of non-security devices. *Houston* states that the display of a scope can comprise "one or more tables, charts, graphs, tree diagrams, or other renderings for presenting data to a user." (*Houston*, para. [0045].) For example, Figure 15 of *Houston* displays a scope in table and chart format. However, beyond this general description of how a scope may be displayed, *Houston* does not describe visually highlighting any sort of symbol corresponding to a group of non-security devices to indicate a number of scopes or events whose source or destination is at any member of the group of non-security devices. Therefore, *Houston* cannot possible teach or suggest the above-bolded features of Claim 1 and the combination of *Ptacek* and *Houston* cannot possibly satisfy Claim 1 as a whole.

The Office Action cites to paragraphs [0042]-[0053] of *Houston*. These paragraphs describe various techniques for managing event data in general terms but do not describe the specific features of Claim 1. For example, according to one technique disclosed in *Houston*, criteria (e.g., a scope) is defined for filtering event data and the result of applying the criteria is displayed in different graphical formats including tables, graphs, charts, and tree diagrams. (*Houston*, para. [0045].) However, Claim 1 does not just require a graph or processing event data. Rather, Claim 1 specifically recites:

> causing display of a first security incident volume indicator on the display that indicates a number of network sessions whose source or destination is at any member of a

group of non-security devices corresponding to a particular group device symbol displayed on the display;

wherein the step of causing display of the first security incident volume indicator includes the step of causing the display to visually highlight the particular group device symbol in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol.

These specific features of Claim 1 are simply not disclosed by *Houston's* general descriptions of presenting analyzed event data or *Houston's* specific illustrations of presenting analyzed event data in table and chart formats. Nothing in *Houston* is equivalent to the claimed "particular group device symbol" that represents "a group of non-security devices". *Houston* has nothing like the claimed "security incident volume indicator" that indicates "a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to a particular group device symbol displayed on the display. *Houston* also fails to describe any mechanism for visually highlighting "the particular the particular group device symbol in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol."

Moreover, there is nothing from the disclosure of *Houston* that indicates recognition of the benefit of visually highlighting a symbol that represents a "hostpot" group of non-security devices so as to simplify the process for the user of tracking down the sources and destinations of a network attack. Simply put, *Houston* does not close the gap between *Ptacek* and Claim 1.

In conclusion, since *Ptacek's* Figure 1 cannot be the claimed "first graph" and since *Houston* does not overcome the deficiencies of *Ptacek*, the combination of *Ptacek* and *Houston* does not satisfy Claim 1 taken as a whole. Removal of the rejection of Claim 1 is respectfully requested.

Claims 18 and 25 recite similar features and are allowable over *Ptacek* and *Houston* for the same reasons.

CLAIM 2

Claim 2 depends on Claim 1 discussed above. Because each dependant claim includes the features of claims upon which they depend, Claim 2 is patentable for at least those reasons that Claim 1 is patentable. Removal of the rejections with respect to Claim 2 and allowance of the Claim 2 is respectfully requested.

In addition, Claim 2 introduces additional features that independently render it patentable over *Ptacek* and *Houston*. For example, Claim 2 features, among other things, "upon user selection of the particular group device symbol, causing display of a second level graph on the display of the computer system." The Office Action equates Figure 2 of *Ptacek* with the "second level graph" of Claim 2. However, Figure 2 of *Ptacek* is simply a patent drawing. Nothing about the patent drawing of Figure 2 suggests that the elements illustrated therein represent "members of [a] group of non-security devices corresponding to [a] particular group device symbol that are a source or destination of any of the network sessions of [a] number of network sessions indicated by [a] first security incident volume indicator", as featured in Claim 2. Moreover, the elements shown in Figure 2 are not in any way caused to be displayed "upon user selected of [a] particular group device symbol" shown in Figure 1 of *Ptacek* which the Office Action equates the "first graph" of Claim 1. Consequently, Claim 2 introduces additional features that independently render it patentable. Claims 19 and 26 recite similar features and are allowable for the same reasons that Claim 2 is allowable.

REMAINING CLAIMS

The pending claims not discussed so far are dependant claims that depend on an independent claim that is discussed above. Because each dependant claim includes the features of claims upon which they depend, the dependant claims are patentable for at least those reasons the claims upon which the dependant claims depend are patentable. Removal of the rejections with respect to the dependant claims and allowance of the dependant claims is respectfully requested. In addition, the dependent claims introduce additional features that independently render them

patentable. Due to the fundamental differences already identified, a separate discussion of those features is not included at this time.

CONCLUSION

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

Please charge any shortages or credit any overages to Deposit Account No. 50-1302.

Respectfully submitted,

Hickman Palermo Truong & Becker LLP

Dated: March 6, 2009

/AdamCStone#60531/
Adam C. Stone
Reg. No. 60,531

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080
Facsimile No.: (408) 414-1076